Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently amended) A method for exchanging a secure cryptographic key for a quantum cryptography apparatus employing non-ideal elementary quantum systems, wherein

[[-]] the apparatus comprises an emitter and a receiver, being connected by a quantum channel and a conventional communication channel,

[[-]] the emitter encodes each bit at random onto a pair of non-orthogonal states belonging to at least two suitable sets,

[[-]] there is ~~no~~ not a single quantum operation reducing the overlap of the quantum states of all sets simultaneously,

[[-]] the emitter sends the encoded bit along the quantum channel to the receiver,

[[-]] the receiver randomly chooses ~~the~~ an analysis measurement within said suitable sets,

[[-]] the emitter sends ~~the~~ a set information along the conventional communication channel,

[[-]] the receiver discards all received encoded bits for which ~~he~~ it has chosen a different analysis measurement incompatible with the set they belonged to and sends an appropriate information to the emitter along the conventional communication channel.

2. (original) The method according to claim 1, wherein in the step of the emitter sending an encoded bit along the quantum channel to the receiver weak coherent states are exchanged between the emitter and the receiver.

3. (Currently amended) The method according to claim 2, wherein the weak coherent states are laser pulses with an average photon number per pulse of less than ~~0,5~~ 0.5 photons, preferably less than ~~0,1~~ 0.1 photons.

4. (Currently amended) The method according to claim 1,

[[-]] wherein the emitter is using two sets $A = \{|0_a\rangle, |1_a\rangle\}$ and $B = \{|0_b\rangle, |1_b\rangle\}$, chosen such that $|\langle 0_a|1_a\rangle| = \eta_a \neq 0$, $|\langle 0_b|1_b\rangle| = \eta_b \neq 0$, and wherein there is no single quantum operation reducing the overlap of the quantum states of all sets simultaneously, and

[[-]] the receiver randomly chooses the analysis measurement between $F_A = \frac{1}{\sqrt{1+\eta}}\left(|+x\rangle\langle 1_a^{\perp}| + |-x\rangle\langle 0_a^{\perp}|\right)$ and $F_B = \frac{1}{\sqrt{1+\eta}}\left(|+x\rangle\langle 1_b^{\perp}| + |-x\rangle\langle 0_b^{\perp}|\right)$ followed by a Von Neumann measurement distinguishing between $|+x\rangle and |-x\rangle$.

5. (Currently amended) The method according to claim 1, wherein after a number of encoded bits has been transmitted, a protocol step is performed, within which emitter and receiver agree on a body of cryptographic key information

~~which~~ that is shared between emitter and receiver, but secret from all other units ~~who~~ that may be monitoring the quantum channel and the conventional communication ~~public~~ channel, or else conclude that the encoded bits can not be safely used as cryptographic key information.

6. (Currently amended) A method for exchanging a secure cryptographic key for a quantum cryptography system employing non-ideal elementary quantum states, ~~where~~wherein

the apparatus comprises an emitter and a receiver, being connected by a quantum channel,

the emitter encodes the key values ~~are encoded~~ on at least two sets of non-orthogonal quantum states, ~~characterized by the fact that~~ wherein it is not possible to find a single quantum operation, whether probabilistic or not, that reduces the overlap of the states of all sets simultaneously,

the emitter sends the encoded bit along the quantum channel to the receiver,

the receiver randomly chooses an analysis measurement within said suitable sets,

the emitter sends a set information to the receiver,

the receiver discards all received encoded bits for which it has chosen a different analysis measurement incompatible with the set they belonged to and sends an appropriate information to the emitter.

7. (Currently amended) A quantum cryptography system employing non-ideal elementary quantum states to exchange secure cryptographic key information and comprising:

[[-]] a source of non-ideal elementary quantum states,

[[-]] an emitter and a receiver, being connected by a quantum channel and a conventional communication channel,

[[-]] the emitter comprising or connected to a random number generator allowing to prepare random non-orthogonal quantum states belonging to at least two suitable sets, wherein there is no single quantum operation reducing the overlap of the quantum states of all sets simultaneously,

[[-]] the receiver comprising or connected to a random number generator allowing to choose an analysis measurement for said quantum states,

[[-]] the emitter being able to send an ~~the~~ encoded bit along the quantum channel to the receiver and being able to send a ~~the~~ set information along the conventional communication channel,

[[-]] the receiver being able to discard all received encoded bits for which ~~he~~ it has chosen a different analysis measurement and to send an appropriate information to the emitter along the conventional communication channel.

8. (Currently amended) The quantum cryptography system according to claim 7, wherein said source is a laser source and the emitter comprises a preparation

device sending laser pulses with an average photon number per pulse of less than 0.5~~0,5~~ photons, preferably less than ~~0,1~~0.1 photons.

9. (Currently amended) The quantum cryptography system according to claim 7, wherein emitter and receiver both comprise processing units being able to perform, after a number of encoded bits had been transmitted, a protocol step, within which emitter and receiver agree on a body of cryptographic key information ~~which~~ that is shared between emitter and receiver, but secret from all other units ~~who~~ that may be monitoring the quantum channel and the conventional communication ~~public~~ channel, or else conclude that the encoded bits can not be safely used as cryptographic key information.

10. (Currently amended) The method according to claim 1, wherein for each bit, the emitter is randomly using one of the four states $|\pm x\rangle$ or $|\pm y\rangle$ with the convention that $|\pm x\rangle$ code for 0 and $|\pm y\rangle$ code for 1, and sends it along the quantum channel to the receiver, the receiver randomly measures σ_x or σ_y, the emitter announces one of the four pairs of non-orthogonal states $A_{\omega,\omega'} = \{|\omega_x\rangle, |\omega'_y\rangle\}$ with w,w' $\in \{+,-\}$ and such that one of the states is the one which ~~he~~ it has sent by sending an appropriate message along the conventional communication channel, the receiver discards all received encoded bits for which the measurement result ~~he~~ it has obtained is possible for both states disclosed by the emitter and sends an appropriate information to the emitter along the conventional communication channel, the receiver deduces the state

actually sent by the emitter and adds the corresponding bit to the key.

11. (new) The quantum cryptography system according to claim 7, wherein the emitter is adapted to use two sets $A = \{|0_a\rangle, |1_a\rangle\}$ and $B = \{|0_b\rangle, |1_b\rangle\}$, chosen such that $|\langle 0_a|1_a\rangle| = \eta_a \neq 0$, $|\langle 0_b|1_b\rangle| = \eta_b \neq 0$, and wherein there is no single quantum operation reducing the overlap of the quantum states of all sets simultaneously, and wherein the receiver is adapted to randomly chooses the analysis measurement between $F_A = \frac{1}{\sqrt{1+\eta}}\left(|+x\rangle\langle 1_a^{\perp}| + |-x\rangle\langle 0_a^{\perp}|\right)$ and $F_B = \frac{1}{\sqrt{1+\eta}}\left(|+x\rangle\langle 1_b^{\perp}| + |-x\rangle\langle 0_b^{\perp}|\right)$ followed by a Von Neumann measurement distinguishing between $|+x\rangle and |-x\rangle$.

12. (new) The quantum cryptography system according to claim 7, wherein for each bit, the emitter is using the related random number generator for randomly using one of the four states $|\pm x\rangle$ or $|\pm y\rangle$ with the convention that $|\pm x\rangle$ code for 0 and $|\pm y\rangle$ code for 1, and the emitter is adapted to send it along the quantum channel to the receiver, wherein the receiver is using the related random number generator for randomly measuring σ_x or σ_y, wherein the emitter is adapted to generate a signal announcing one of the four pairs of non-orthogonal states $A_{\omega,\omega'} = \{|\omega_x\rangle, |\omega'_y\rangle\}$ with w,w' $\in \{+,-\}$ and such that one of the states is the one which it has sent by sending an appropriate message along the conventional communication channel, wherein the receiver is adapted to discard all received encoded bits for which the measurement

result it has obtained is possible for both states disclosed by the emitter and sends an appropriate information to the emitter along the conventional communication channel, wherein the receiver is adapted to deduce the state actually sent by the emitter and adds the corresponding bit to the key.

13. (new) The quantum cryptography system according to claim 7, wherein the transmittal of an encoded bit along the quantum channel from the emitter to the receiver comprises an exchange of weak coherent states between the emitter and the receiver.